Executive Panel Session:
Combatting Financial Crime in a Digital Age

Opening Remarks:

Ian Gorst
Minister of External Affairs, Government of Jersey

Panelists:

Abdul Rasheed Ghaffour
Governor, Bank Negara Malaysia

T. Raja Kumar
President, Financial Action Task Force (FATF)

Cecilia Skingsley
Head, BIS Innovation Hub, Bank for International Settlements

Moderator:

Jennifer Elliott
Advisor, Monetary and Capital Markets Department, IMF;
Board Member, Toronto Centre

Date:

Apr. 17, 2024

Transcript:

Babak Abbaszadeh:

Good morning, everyone. Welcome to Toronto Centre's Executive Panel on Combating Financial Crime in a Digital Age. My name is Babak Abbaszadeh, I'm the President and CEO of Toronto Centre, and we've been in the business of supervisory training for the past 26 years, having trained 26,000 financial supervisors in 190 countries and territories on financial stability and inclusion. Today's conversation is very timely and very important from a global perspective. Financial crime is a very distorted force, and it affects everybody: citizens, rich and poor countries, and institutions. As criminals are becoming more sophisticated, technology is also helping them. So, to combat that, it requires a big ecosystem, supervising authorities are involved.

So, we have put together an esteemed panel for you, and you have seen their names, Abdul Rasheed Ghaffour, Governor of Bank Negara Malaysia, and I was delighted to find out that prior to my arrival, he was a Toronto Centre participant, so he's an alumnus, so that's great. We also have Mr. T. Raja Kumar, who's the head of the Financial Action Task Force, and our dear friend Cecilia Skingsley, who's the head of the BIS Innovation hub. Of course, this panel is being moderated once again by our board member, Jennifer Elliot. She does such a good job that we keep bringing her back. So, Jennifer, it reminds me of when I was a kid and I did a lousy job of washing the dishes, so my mom never asked me to do it again, but you keep doing well.

Before we start though, I would like to ask our special guest to come and deliver brief opening remarks. We have the Honourable Ian Gorst, who's the Minister of External Affairs of the State of Jersey. Jersey Overseas Aid is a big funder of Toronto Centre. In fact, some of our combating financial crime programs are sponsored by Jersey Overseas aid. Mr. Gorst was elected to Parliament in 2005 and he's held a variety of positions such as Senator, Minister of Treasury, Natural Resources, Chief Minister, I'm not sure what else is left, but he's done all those jobs. So, may I ask you to please come and provide your brief remarks? Thank you.

Ian Gorst:

Thank you very much indeed. It's a real pleasure for me to be here again, joining you this morning at this really important event. I'm always reminded when people read my CV out that my political opponents would say I'm trying every job, and I haven't yet found one that I'm very good at. This event this morning for us in Jersey and being associated with it is really because we value greatly the excellent relationship that we have with the Toronto Centre, largely through our aid agency, but also with our regulator, the Jersey Financial Services Commission. Jersey is an international finance center with links to over 200 jurisdictions. That, of course, exposes us to a variety of evolving financial crime risk, and combating financial crime is a major focus of Jersey's government and has been of the roles that I've carried out in government, and of the relevant agencies that we have in Jersey, especially now, and I have be careful how I say this, that we come to the end of our MONEYVAL assessment, that's the European Council body that assesses in regard to compliance with FATF recommendations, and the results of that will be announced in July of this year.

In recent years, we've done much to revise and update our systems to ensure that they are fit for purpose, such as bringing all nonprofit organizations into scope of regulation and creating a dedicated sector supervisor. We've introduced new legislation to make it an offense for anyone to fail to prevent money laundering, putting renewed onus on those who are practicing in the financial services industry. We've put into law civil financial penalties for significant and material contraventions of our money laundering order and the regulator's code of practice. We've created deferred prosecution agreements which allow entities to submit a self-report on any breaches of the money laundering order, or the codes of practice. We continue to update existing national risk assessments and author new ones in developing areas such as an upcoming publication on our small virtual asset sector.

An advantage, of course, of being a relatively small jurisdiction is our ability to respond to global events quickly. We've shown that in our response to the Russian invasion of Ukraine. But, in responding with a strong sanctions provision, we know through experience that there's always room for improvement and we must continue to monitor evolving work around sanctions evasion and ensuring that those sanctions are actually working. The use of asset recovery agreements is also an important initiative for Jersey. In recent years we've worked with recipient jurisdictions to identify, confiscate, and return illicit funds to countries including Nigeria, Kenya, South Africa, and Mozambique. We are fully aware in Jersey that combating financial crime, terrorist

financing, and proliferation financing is something that we have to do together, and that is why I'm particularly pleased that the Toronto Centre will be doing an event in the autumn with our financial services regulator focusing on the challenges of effective supervision relating to financial crime, but also looking at capacity building.

We are grateful to the Toronto Centre because what we find is in helping us support that capacity building and thinking about appropriate supervision, and particularly as we see in the digital age, we learn and we strengthen our system as well as those from around the world that might come along and learn from our system as well. We find it to be mutually beneficial. The more cooperation domestically and internationally we have, the harder it will be for criminals and terrorists to abuse our financial markets. And therefore, once again, it's a great pleasure for me to be with you and to join you and I'm remain extremely thankful to the Toronto Centre for all their work. Thank you,

The more cooperation domestically and internationally we have, the harder it will be for criminals and terrorists to abuse our financial markets.

Ian Gorst
Government of Jersey

Babak Abbaszadeh:

Minister, thank you for those insightful comments. It comes kind of like a mini case study for this panel, and also your kind remarks about Toronto Centre. Jennifer, over to you. Thank you.

Jennifer Elliott:

Thank you. Good morning, everybody, good morning to the panel. It's great to be here. So, we're going to dive right in because time is short, and the topic is huge. Raja, we're going to start with you.

So, you're the head of an organization that leads the global fight against the use of the financial system for criminal proceeds, for crime, and you put out a report in November on Illicit Financial Flows from Cyber-Enabled Fraud. Can you give us a sort of big picture of the scale and the nature of what's going on out there in terms of financial crime and what do we mean by cyber-enabled fraud?

T. Raja Kumar:

Yeah, sure. Hi, morning everyone. The challenge before us is a huge one. Criminals are very quick to exploit opportunities, and what we saw during the COVID-19 period essentially was criminals taking full advantage of the opportunities supported by technology, by cyberspace, to basically commit cyber-enabled fraud at a scale that is unprecedented. You're talking about countries that are reporting their citizens losing, in smaller countries, low billions of dollars, and for larger countries, multiples of that. So, it just gives you a sense of the scale and the magnitude of this problem. This is not going to go away soon. I'll say the trajectory of the threat and the risk continues to rise because criminals are seeing this as a wonderful opportunity to make quick money exploiting the fact that you are basically traversing jurisdictions at the click of a button, and fully exploiting the space that is left when there is insufficient national effort that is put in, and when you have a lack of international collaboration that is sufficient to tackle the nature and scale of the problem.

So, during the Singapore presidency, we basically identified this as very much a contemporary risk, a growing risk, and something that needed to be looked into, which is why we said we needed to study exactly how the funds flows are happening in relation to criminals moving their monies to safe spaces to then enjoy the fruits of the crime. When we take a look at the nature of this threat, we are seeing this happen on an industrial scale. You are talking about literally scam factories that have been established in different parts of the world that are targeting citizens.

Some people think of this kind of crime as victimless crime. Actually, when you talk about this crime, there are victims who are suffering as a result of say some of the internet "love scams" where they have been decimated of all their life savings. So, you are seeing hopes and dreams dashed. You are seeing lives even put at risk because some of the victims become suicidal because of the prospects being very dim in the future with no kitty that they can essentially lean on for the rest of their lives. This is a serious problem, and it impacts people, it impacts lives, and so, we are essentially turning the spotlight on this area. We are asking governments to take a close look at it, and better appreciate what the risks are, and what they need to do about it nationally, regionally, and then globally. On the global side of it, FATF has again turned our attention to the illicit proceeds of prime, and I'm firmly convinced that we need to be very targeted and very deliberate about going after the proceeds of crime in this area because when you cut off the floor of money to criminal enterprises, go after their assets; you essentially debilitate criminal enterprise, you prevent them from mounting even more ambitious operations, you are actually making sure that they don't have the funds to buy the latest technologies, which make it even more difficult for law enforcement to tackle this problem, and there's also a very real risk of subversion of the rule of law and of compromising of officials to corruption.

> It is not just about the financial institutions and the central bank. It is about a whole of society approach that needs to kick in to be effective in the fight against this very challenging crime.
>
> **T. Raja Kumar**
> Financial Action Task Force

So, this is a pernicious area and I think we would do very well to focus a lot more attention on it and tackle it, as I mentioned, nationally, regionally, and globally. At the national level, it really would take a whole of government perspective to deal with it. It is not just about the financial institutions and the central bank. It is about a whole of society approach that needs to kick in to be effective in the fight against this very challenging crime.

Jennifer Elliott:

Thank you. That's a great segue to the governor because we can put it to him. I did wonder, on top of monetary policy and bank supervision, how did you become in charge of financial crime in Malaysia? know you're not in charge, but this is a great lead in, it's a whole country effort. Tell us how it's going in Malaysia and what you've been doing in Malaysia and what the role of the central bank has been in that.

Governor Abdul Rasheed Ghaffour:

Thank you. Thanks Jennifer and thanks everyone for being here today and my fellow panelists and Babak for the opportunity to share our experience here. I think as what has been mentioned by both Jennifer and Raja, I think the whole of nation approach is very important. That's how we take it. How we got into this is because the financial sector has always been used as a conduit

for these cyber criminals. So, that's where I think we have the responsibility in terms of ensuring the stability and confidence of the financial system, that's where I think we were at the central stage, but this goes beyond the central bank. So, that's where I think what we have done is adopt a whole of nation approach where all segments of society, all segments of the government are actually involved in terms of managing this issue.

Let me just start by saying that we know that financial fraud is a global issue, and criminals are now increasingly using sophisticated matters and especially leveraging on the technology to defraud victims. As we enhance, the adoption of digital finance increases, and criminals are also finding new and innovative ways to commit financial crimes. In fact, they're always ahead. They try to be ahead of the regulators and sometimes I think they're even a few steps ahead of us. The overall losses that we have seen from this fraud, while it's troubling, have remained relatively small in case of Malaysia. But if you look at them, especially when we compare them in terms of the volume of transactions processed to our financial system, it's rather small, but it is a very important issue. Why? Because the - significance of one single case can have an impact in terms of the confidence on the system itself.

> In prevention, the bank continues to issue relevant regulations related to scams, covering the areas of preventing scams, and protecting the consumer.
>
> **Abdul Rasheed Ghaffour**
> Bank Negara Malaysia

That's where I think it's very important for us to really step up our measures in terms of addressing this. Let me just touch on the terms of the approach we are going to take. I think we need to adopt a whole of nation approach to combat financial crimes, especially the online financial scams. This comprises of a three-prong strategy. Number one, in terms of prevention, second, in terms of recovery and enforcement, and third, in terms of creating awareness. Let me just touch briefly on these three areas. In prevention, the bank continues to issue relevant regulations related to scams, covering the areas of preventing scams, and protecting the consumer. Meanwhile, on the telco side, this is a very important stakeholder that we need to also manage because their products are what is being used for financial crimes to happen. So, they have to come in and play a role as well. Regulations have also been issued by the Communications & Multimedia Commission related to scam or malicious content such as taking down or terminating suspicious telephone numbers and internet content.

That's where I think it's very important approach, not just the central bank, not just the regulators and supervisors, but also in terms of the Malaysian Communications & Multimedia Commission. Briefly in terms of recovery and enforcement, we have the Royal Mission police that plays a very active role here, and they apply a multiple enforcement approach to eliminate the scams indicate through various operations and money laundering investigations. This has led to prosecution of the perpetrators and returning of the fines to the victims. We need to really show examples of how this works to make sure that we can really kill off the intention or the incentive for them to commit this crime. These actions are mostly supported by the NSRC or the National Scams Response Center that we have set up, and this involves not just the police and central bank, but also the private sector and the FIU through timely information sharing and detection of scam events.

Quickly on awareness, the government agencies, and the private sectors, like the banking sector and the telcos, have coordinated efforts in educating the public through the various channels and platforms while leveraging on our own resources capabilities. So that's also a concentrated effort together. The awareness content is tailored, based on the latest trend identified by the authorities, and developed to cater to different types of communities as well. For example, we have seen Mr. Raja talk about the love scam, and in terms of other scams, opportunities to work elsewhere. We also have a lot of investment scams and sometimes during certain festival festivities, we see different kinds of scams coming into play. So, that's why I think we are more targeted in terms of how we educate and create awareness, and that's why I think the approach that we have taken is the whole of nation approach and then focusing on prevention, recovery, and awareness. I'll stop here for now. I'll come in later on in terms of sharing a bit more details on all these three areas as we go to the Q and A session.

Jennifer Elliott:

It's really striking how you put it right? Criminals are really clever and play on human emotions and this is really difficult to think about; love scams, festivals, and all these sort of things. They really play on the human identity to keep going, but of course they're using technology, which is where we are, which takes us to Cecilia. So, Cecilia, industrial scale was the other thing that Raja said that really was striking because industrial scale sounds really daunting and at the BIS innovation hub you're thinking about technology, the landscape, how it's shifting and it's shifting fast, and both of you have said that as well. So, how does the Innovation Hub look at the challenge of this? And maybe you can mention a project you have, Project Aurora, to set us up for how technology might help or how those who are watching the technology can see what's evolving.

> It's all been laid out: how technology is used for bad purposes. So, it takes technology used for good purposes to beat the bad.
>
> **Cecilia Skingsley**
> Bank for International Settlements

Cecilia Skingsley:

Okay, thank you very much. I'd like to just build upon some things that some of the panelists, the panelists have already talked about when it comes to the landscape and then I'll talk a little bit about how we think of possible solutions. I think it's striking that are not in a very good equilibrium here, because a lot of the enforcement to combat this now sits within the banks. But the banks can only analyze data in silos. They can't share their findings. It's very difficult to see these networks really that we are having. The high penalties for failures leads to very high levels of over-reporting. Taking this country (the United States), 3.6 million SARs (suspicious activity reports) were filed two years ago and it's increasing every year. The compliance costs are huge: 274 billion in 2022, also rising year after year. And you can compare them to 74 billion with only something around between 2 and 5 billion that actually recovered, so the payback, or the return on these investments is very unimpressive and we can also see the macro consequences of this: banks de-risking, making financial inclusion, and increasing problems.

That's the steady state and it's all been laid out: how technology is used for bad purposes. So, it takes technology used for good purposes to beat the bad. FATF, you have been onto the issues around using novel technologies to beat this and has been a great inspiration for us in the Hub. So, coming to Project Aurora, which has been done in the Nordic Center, it's still going, and we are progressing now with the private sector, but it's in essence, using the latest in artificial

intelligence, doing network analysis, and combatting the fact that banks have this very limited knowledge. You can do these things now; you can share data while actually not really sharing it, and importantly, we can apply some privacy and housing technologies, so we don't have to look into what individuals are doing. We can still find a lot of time, a lot of interesting findings.

So, what are the findings then? Well, we found that we could reduce 80% of the false positives so we can bring down the reporting avalanche and different kinds of complex money laundering schemes could also be found. Building on this, we hope to take it to a proof of concept, and it takes public and private collaboration to get anything done. I can get back on the details of that. Two more projects I'd like to highlight. Project Hertha, we're going into instant payment systems there. We want cross-border payments to work better in the world. Connecting instant payment systems is one very promising way to do that, but in order to not make the risks even higher, you have to use technology. Last but not least, compliance checks. I think we're all grumbling about these things. Project Mandala is about using what we call common protocol layer technology to build in automatically whatever regulatory and policy measures that need to be in place when people want to do transactions. So, sanction screening, fraud screening, AML, and capital flow regulations. Technology can get a lot of good things in place, but there are some frictions getting that done, but I'll come back on that.

> Criminals operate at the speed of money. Law enforcement operates at the speed of law, and there's a disconnect between the two.
>
> **T. Raja Kumar**
> Financial Action Task Force

Jennifer Elliott:

Okay, thanks. I mean, I was a bit worried at the tone of the panel until you gave us a little bit of optimism at the end. I really love the line, "Good technology to deal with the bad." We are in the cyber landscape that we're in, it's not going away. We all enjoy the positives of it, so it's about the negatives. So maybe I have a few questions about how we can coordinate better. Raja, I have two questions for you. I wanted your thoughts on how policy makers globally and regulators and supervise coordinate better, but also to Cecilia's point about bringing costs down, how do you guys think about that in FATF standards and in the global coordination? How do you think about bringing costs down, and we have to combat the problem, but it's expensive to do. So, how do we balance those things and how does coordination help?

T. Raja Kumar:

Okay, let me deal with your first question. So, what ought the global response be to tackle this high order challenge, which is not going to go away anytime soon? There's a quote that I've been using recently "Criminals operate at the speed of money. Law enforcement operates at the speed of law, and there's a disconnect between the two." So, what is needed really across the globe would be faster, more responsive policies, systems, and frameworks to tackle this challenge. We really have to look at this at the national level. Governor Ghaffour has mentioned that it has to happen at the whole of society level. You're not just looking at the traditional players that you would engage, but you have to take a look at the telcos and the online market sellers. There's a whole ecosystem out there that needs to be brought on board to then mount an effective response to this major challenge that we face. That is at the national level.

Then, when countries start upping their game and making themselves more resilient, criminals are very quick to move and look for the next weak spots, and you could then see a displacement to another country in the region, which is why at the regional level as well, that strategic conversation needs to happen. Regions as a whole need to up their game, put in place robust policy systems and infrastructure to essentially tackle the challenges that are posed. Then, at the global level there's also work to be done. We just had in London, two weeks ago, a Global Fraud Summit that brought together countries. It was an effort really to illuminate the problem and take a look at how governments are essentially responding to the challenge. In the process of doing that, you actually highlight best practices that others can quickly learn and then up their game to be more effective. This is the kind of response that is needed.

> All of us here, on your cell phone, you are just one click away from being compromised, one click away from someone essentially taking control of your phone.
>
> **T. Raja Kumar**
> Financial Action Task Force

But I think we also have to think about global architecture that right now is not quite in place to tackle the fraud situation, which is again, trajectory wise, going to continue rising until there's a very definite and strong and decisive pushback against it to tackle it in a far more effective way.

One of the points that Governor Ghaffour actually raised is a pretty fundamental one. I think not enough attention is being paid to it. All of us here, on your cell phone, you are just one click away from being compromised, one click away from someone essentially taking control of your phone and then knowing everything about your transactions and then being able to commit fraud. So, I mean if you think about the nature of that risk, you being one click away, everyone is a potential victim, which is extremely scary. Which goes then to this whole concern about trust, that this undermines trust. Because when you see a message now coming from your bank, you are asking yourself, is this really from the bank or not? I mean you should be asking that question, by the way, because we need to have healthy skepticism when taking a look at some of this, and then doing your necessary due diligence and verification. But that is the nature of things now, such as the threat. And so, my call to action is for countries to take this very seriously, protect their citizens because this is hurting people, hurting lives, and hurting aspirations. Globally, I think we have to do more to tackle it because otherwise criminals will continue to build this space and they're very quick to do just that.

Jennifer Elliott:

It's very interesting the way you described the coordinating problem. You went quickly past the cross border, which we'll come back to, but it's more than that, right? You're asking for financial regulators to be talking to media regulators, to be talking to law enforcement. This is difficult, right? This is difficult, but the scale of the problem demands that kind of a response.

T. Raja Kumar:

Which then goes to the second part of your question, in relation to this whole issue of cost and specificity. The challenge is for us to get better quality STRs (suspicious transaction reports), SARs, there has to be a lot more engagement by the financial intelligence units with industry so that you have a better, more accurate shared understanding of what the challenges are. Then

the financial institutions, for example, can be more targeted, more focused on what it is that they're looking for. I also agree, that in terms of protocols and in terms of enabling systems, you need to have a lot more sharing of information including across financial institutions because it is terrible, it'll be a travesty if one financial institution thinks that something is horribly suspicious but can't share this information with your other banks. So, there are some examples now globally where we are seeing legislation being put in place that enables just that. So, in Singapore there's Project Cosmic, which is well underway and there are other initiatives that are now at the national stage, and I would ask everyone to take a look at how these progress, and the fruits that they bring to help us to be more effective in the fight against financial crime.

What we have done is establish a National Fraud Portal (NFP) at the national level, and this portal is set to be launched by the middle of this year. In terms of what it does, this will also further enhance in terms of the NSRC's (National Scam Response Centre) tracing capabilities and thus reducing the fraud losses

Abdul Rasheed Ghaffour
Bank Negara Malaysia

Jennifer Elliott:

That's great, thank you. It's such a huge issue. So, let's take some of your challenges to the Governor. But first, I wanted to ask you a little bit about coordinating cyber-attack and the quintessential sort of cross-border problem and how that's happening in your region, but then going to Raja's challenge, what do you think we can do to be smart about compliance costs and making it more effective? We know the scale of the problem, it has to be tackled, so how do we do it effectively? It's a little bit of a blend of Cecilia's challenge as well and using technology.

Governor Abdul Rasheed Ghaffour:

Alright, thanks Jennifer. But before that, let me just go back to the early question because I missed this point. I think Cecilia touched on the use of technology and utilization, I think just to share in terms of our experience, we also make greater use of technology to enhance our enforcement capabilities and detection. What we have done is establish a National Fraud Portal (NFP) at the national level, and this portal is set to be launched by the middle of this year. In terms of what it does, this will also further enhance in terms of the NSRC's tracing capabilities and thus reducing the fraud losses. The NFP will be harnessing the power of data analytics to support faster tracing and also analysis. The NFP is also exploring embedding predictive analytics, enabling the NSRC to identify suspicious account flows and potential connections to mule accounts.

But just one point to share: when this is in place, it will leverage on the capabilities of shared payment network among the FIs within the country. This will go back to your question of, "How do you reduce the compliance costs?" So, the sharing of infrastructure and platform is critical. So that's where, in our case, we have a shared platform because we have PayNet, that is the infrastructure provider for payment systems which is owned by the central bank and the industry. So, that's where the infrastructure is being shared. So, that's one way you can reduce the cost for addressing and managing this fraud activity.

Secondly, going back to the NFP, while leveraging on the shared payment network among the FIs within the country where all the affected FIs will be alerted once the fraud incident is triggered, and when fraudulent funds are passed through with their bank accounts, so it's

automatic. The FIs will then respond to this alert by holding the funds for due diligence and then updating the account status or information. Subsequently, the law enforcement agency will be notified for their formal enforcement actions. This is expected to reduce the time for conventional fundraising, which normally happens within a few weeks to just below five minutes. So, that's a very powerful tool, a portal that can really help in terms of tracing and also reducing losses from fraud.

Going back to the point on cross border; I think it's something that we are pushing forward. I think we are part of the nexus, like the BIS Innovation Hub. We want to promote cross-border payment leveraging on the digital payment infrastructure as similar to the national approach where it's important that it's a whole of nation approach.

> We all know that the public sector is suffering from resource constraints and if they don't have the right data infrastructure and the ability to share information or have the right collaborative analysis models, they get a bit stuck.
>
> **Cecilia Skingsley**
> Bank for International Settlements

We do see the importance of having a whole of region approach, in this case. Perhaps, I think more globally in terms of our coordination effort and our collaboration effort in terms of managing this fraud. It is very critical and one example that we are doing at the regional level, in the case of ASEAN, we participate in the ASEAN Digital Technology Network, the cybersecurity resilience information sharing platform, or we call it, the CRIS. So, that's where the sharing of information happens. This platform actually brings together central bank members from the ASEAN countries at least once a year to exchange cybersecurity information and collaborate on capacity building initiatives. But moving forward, there could also be some kind of on-the-spot kind of motus operandi so that people get a little bit of the information themselves. We also remain committed to strengthening the strategic bilateral collaboration with relevant regulatory authorities internationally, particularly in the areas of cybersecurity information exchange and capacity building initiatives. This is very important because the weakest link can be the greatest source of risk to you. So, whoever participates in the cross-border platform, you need to make sure that the capacity building is there, and everybody has the same level of awareness and standards in regard to compliance, and also in terms of ability to manage this potential cyber security threat.

Jennifer Elliott:

It's interesting that you say capacity building, because it's a little bit like what Raja just said as well. I mean, a weak link is a problem. We all know from when we have those phishing tests from our IT department, it's probably pathetic how many of us. So, in some sense, our behavior is also changing and it's catching up a little bit, but it's very interesting that you use the word capacity. I think sometimes financial regulators forget about other agencies' capacity and so on. So, a super important point. Okay, Cecilia, you brought up the level of optimism last time, but maybe you could talk a little bit more about what you see that regulators and supervisors should be doing and should be using technology for, and how they can do a bit better in that regard.

Cecilia Skingsley:

Okay, I'd love to. Well, first of all, we all know that the public sector is suffering from resource constraints and if they don't have the right data infrastructure and the ability to share information or have sort-of the right collaborative analysis models, they sort of get a bit stuck. You can

basically build whatever you want with technology these days, so I think Aurora is a very promising initiative, as I mentioned, you should have a look at it if you haven't done it already. We have detailed information on our website, but you have to go much further than that. My staff has put together a long list of a lot of technical stuff we could do, but let me talk about something else which I think is very important in this group. We've also talked with the supply side of SupTech tools in the private sector and the demand side, namely supervisors. And we can see that there is a clear disconnect here.

The SupTech industry is not very profitable, it's quite a small industry, so if we really want to have the best of the best from the private sector build things for us, we have to be much better procurers and collaborate across.

Cecilia Skingsley
Bank for International Settlements

Jennifer Elliott:

Just before you continue: SupTech - supervisory technology, so the use of technology by supervisors.

Cecilia Skingsley:

Exactly. Thank you very much for that clarification. There's a lot going on in many supervisory authorities and law enforcement agencies, but it's mostly about just automating what's already there. It doesn't really sort of scale beyond that. There are some interesting experiments going on in different places, but it seems like it's all more or less stuck in what I call prototype hell. It's really hard to take it into full implementation, and, ladies and gentlemen, scale it across to other authorities. There are just too many impediments there. And to add further to the insult, I'm going to be a little bit negative, well, I promise I'll stop on the optimistic side, the public sector is not seen as very impressive buyers of SupTech from the vendor side. So, half of the vendors that we talk to say they took unclear objectives, challenging costly procurement rules, and the SupTech industry is not very profitable, it's quite a small industry, so if we really want to have the best of the best from the private sector build things for us, we have to be much better procurers and collaborate across.

So, the tech is there. Implementation, well, there's still room for improvement there. Our job at the Hub is by experimenting and building things together with public sector, and we have many central banks partnering up in our various projects around this, but also bringing in the vendors, we hope not only to demonstrate the art of the possible when it comes to technology, but also raise the general level of mutual trust so that someone on the public sector side can tell someone on the commercial side, "This is my problem, these are our vulnerabilities, what can you do to help us find a solution to this?" So, we need much clearer paths to collaboration, public and private sector, but mostly what I think is that we need to have clear paths to production. We know what is needed and we know what the technology can give us, but we haven't sort of laid out the way, but there's ways to do that so I'm sure we'll get there.

Jennifer Elliott:

So, technology has to be integral to the solution as well as coordination, but there are some huge challenges in putting that in place.

Cecilia Skingsley:

I would call it teething problems, but we need to talk about those as well.

Jennifer Elliott:

Raja is dying to say something.

T. Raja Kumar:

Yeah, I am. Just three points from just listening to my fellow panelists: the first one is I think there are signs now that we are mounting a more effective global response. On the FATF side, maybe I can just share some of the recent standards changes that we have made that will actually help national authorities and law enforcement around the world be far more effective with the fight against financial crime.

The first one was actually the changes that we brought about to the beneficial ownership transparency area. This allows national authorities to essentially lift the lid and take a look at who exactly is controlling shell companies and other corporate entities, right? Under the Singapore presidency we've extended this requirement to also cover legal arrangements such as trust. So, a huge change I think on the global standards front, and this is then coupled with the major change that we have made in relation to asset recovery standards.

> I think there's tremendous potential for us to really, fully mobilize technology to be more effective in this fight against financial crime. But there are some real tough challenges that actually exist within that space.
>
> **T. Raja Kumar**
> Financial Action Task Force

We've put in place already a new FATF standard that would require national governments to put in place national laws that would equip their law enforcement with a far wider suite of tools, legal mechanisms, capabilities to go after the dirty money, and essentially, be more effective in taking that away. Combined, there's actually tremendous synergy between these two in operation, I think there's tremendous potential here. So, watch this as it essentially moves from the early stage, which is where we are. Once countries have fully operationalized it, we ought to see a movement of the needle in terms of effectiveness.

The second point was something that was mentioned by Cecilia in relation to national authorities being resource constrained. Someone at a major conference not too long ago made a very cutting remark that when you put all the analysts who are looking at financial crime from the major banks, that this actually dwarfs a lot of national capabilities. What this means is that we have to work a lot more closely with the private sector to make full use of their capabilities, share more, and be more effective together when you collaborate. So, this sounds obvious, but it's incredibly hard to do and it's got to do with trust and building that trust, step-by-step and then scaling it from there.

The final point I'll make is in relation to the use of technology, I think there's tremendous potential for us to really, fully mobilize technology to be more effective in this fight against financial crime. But there are some real tough challenges that actually exist within that space. The key one is balancing the different aspects. You've got privacy, you've got cost, you've got the need to share, and the need to enable the sharing of information. These are actually playing off against each other and each society will have to decide what is the appropriate calibration of your actual laws to find a way forward amidst all of this. Not an easy challenge.

Jennifer Elliott:

Okay. Cecilia has provoked the governor also for a response, so we'll take a couple of comments from you and then we'll open up the floor. So, think of your questions now.

Governor Abdul Rasheed Ghaffour:

Thanks Jennifer. I think just to respond to what Cecilia mentioned in terms of trusted platforms, I think it's very critical for industries to share information, and I think Mr. Raja took it to a global level. How do we have this kind of platform where we can share information addressing privacy, and what are the data constraints? Just to share at the national level, what we have done is that perhaps I think this can also be done at a regional and perhaps a global level. We feel this is important, especially in the scenarios where one FI is tech, or compromised by exploiting vulnerability that is also present in other parts. So, that's very important.

What we have done is that to minimize its contagion risk, we established something we call FinTIP. FinTIP is the financial sector, cyber threat intelligence platform. We did this in 2021 to serve as a trusted platform for collecting, aggregating, analyzing, and disseminating cyber threat intelligence within the financial industry. This can always be expanded at the regional and global level. Right now, I think the FinTIP is comprised of 40 major FIs, electronic money insurers, and financial market infrastructure operators, such as our PayNet, as members and with the ongoing objective for progressively onboarding the remaining FIS in the face approach. What happens is that through this FinTIP platform, participating FIs can quickly exchange a cyber threat in information and enhance collective preparedness to potential system wide effects. So, I think that's very important.

Jennifer Elliott:

Thank you. Yeah, there are many questions for you on that, but let's go to the audience for questions for our panelists; you have a lot of expertise up here on financial crime, especially provocative questions if there are any.

Audience Member:

Well, thank you. As I was thinking about my questions, as the moderator, you asked most of them and as the panelists, you spoke to many of them even in advance of my thoughts. But one of the questions I had was, I didn't hear anybody mention two things. One was GFIN, whether the Global Financial Innovation Network is a catalyst for bringing SupTech and RegTech together in the marketplace and whether you've engaged with them. And the other question I had is, are tax shelter havens still contributing to the extent that they were to the nature of the opacity of financial markets? Thank you.

Jennifer Elliott:

So, in your last question, you're asking about opacity of transactions rather than who's housing the industrial scale criminal outfits. Correct? Yeah. Great. I am still stuck on the industrial scale, part, that's just amazing to me. Who wants to take GFIN? Cecilia?

Cecilia Skingsley:

I don't know, but I have a hundred members of staff so I'm sure someone has been in touch with them. Thank you for the encouraging comment. We'll definitely look into it. We need all-hands-on-deck we can find jointly.

Jennifer Elliott:

I'm going to ask Raja about the offshore central tax haven. Unfair broad brush of that question. Not the way I put it, not the way you put it, but do we still have a transaction transparency problem in the world that we once had?

T. Raja Kumar:

As I look ahead, we are about to start the next round of FATF mutual evaluations and one of the things I would ask everyone to look at is the outcome of that particular exercise, because we are. In this round, the major change would be that we are looking very specifically at the risk and context of each jurisdiction, and establishing to what extent each jurisdiction fully comprehends and fully understands its risk and context, and what they're doing about it to effectively mitigate these issues. So, it's a very sharpened focus on this and this area would be one of those obviously that would be looked at.

The second thing is in terms of specificity of the recommendations that are made by the evaluating teams so that countries can be very focused in what it is that they target in their action plan, and with a six year mutual evaluation round, this is a very ambitious effort on the part of FATF, but it also means that for global institutions, they will have access to fairly recent information. So, I think that's something you have to look forward to. It's a high order challenge, by the way, for us, but we have collectively decided, and are embarking on this.

Governor Abdul Rasheed Ghaffour:

Just to touch quickly on the GFIN, thanks so much for raising this. I'm not sure at the regional level, I believe there's some collaboration with GFIN, but if not, I think we'll certainly take it up. Secondly, in terms of the capacity operations, I think the principle that's important is number one, transparency. Secondly in terms of disclosure, and third I thought is in terms of sharing of information, but what's more important is that not just about sharing, but the quality of information and timeliness of the sharing of information. That's very critical. So, that will definitely enhance our ability and capability to address these potential fraud's coming.

Jennifer Elliott:

Oh, fantastic. *Points to audience member*

Audience Member:

Good morning, everyone. From the insights of the panelists, I have understood that there is a lot of work that has been done across the globe, but I'm wondering is there any organized streamlined platform, maybe led by the IMF or the World Bank, that can also reduce the compliance cost where countries can pool their funds and maybe the infrastructure can be made from there and it can be applied to specific regions or countries in that way including Africa and the Middle East. So, is there any organized, agreed upon framework?

Jennifer Elliott:

So, I think your question comes down to the reality for low-income countries, which is the cost of, it's not just the compliance cost for financial institutions, but just the cost of keeping up with technology. The cost of coordinating across the border is pretty prohibitive. Correct. So, what are we doing about that? I mean the answer on the IMF side, and I believe the World Bank side, I do know for example, the World Bank has just started a project in the Pacific Island countries to try and do exactly this. So, where you see it's a scale problem for cross-border payments,

where you have a lot of very small countries who are at risk because complying with AML/CFT and investing in technology is difficult, but I think that's very nascent. I know at the Fund we don't do that, but it's a good question: is there a way to scale, platform wise, so that low-income countries can benefit from joining up, so to speak, with a communal approach that reduces costs for each of them? From what I know, and you guys can react, from what I know one of the difficulties is that law is national, and many changes need to be made nationally and compliance still remains national. So, building that trust to build a platform can be very, very difficult. But maybe the panelists want to take a shot at what we are doing for low-income countries in terms of helping them access technologies.

> One of the difficulties is that law is national, and many changes need to be made nationally and compliance still remains national. So, building that trust to build a platform can be very, very difficult.
>
> **Jennifer Elliott**
> IMF; Toronto Centre

Cecilia Skingsley:

I can just say that there is clearly a deficit of public goods services in the digital era. I mean, when you're looking at the headline of this: Combating Financial Crime in a Digital Age, that's very fundamental things about how does public sector work, state legislators, and what is the offer they give to its citizens? We are all very excited about everything that a digital society gives, but it has a very, very large dark alternative side that we try to address at the same time, and we can't keep up. I think it needs much more effort. The IMF, the BIS, and the World Bank need to provide sort of what I call public goods off the shelf. We try to do our best from the BIS Innovation Hub. We don't have the mandate to launch our things for others to use, but it's there for others to pick up and be inspired by. But I think a much more consolidated effort is really needed. So, thank you for raising that.

Jennifer Elliott:

Okay, thanks. I have a question, because you raised AI and everybody else just let it go, but you have started to explore that space and the BIS Innovation Hub. But I have a question for all of you, is it a plus or a minus, or do we know yet how AI changes this? The first people to innovate are the criminals, you've all said that, and AI is new and now we can all open ChatGPT and have a go. How devilish is that for us and do you see it, on the whole, as a positive in the sense that the technology would then be available to everybody to combat the problem?

T. Raja Kumar:

This is a major challenge I think, but the way to tackle it is essentially governments and others also investing in this to counterchallenge. If you think about deep fakes and someone essentially replicating your voice, replicating your image, and even talking to your relationship manager at the bank, this brings shudders down many spines, I think. And so, we need to counter it. So, what's important from a FATF perspective is understanding the risk. It always starts with understanding the risk. Then, the quick next question is how do you respond to it? I don't think we are in this alone, there's a lot of cross-learning that we need to have across countries and across tech providers as well. We should be talking about contemporary issues

and challenges and what we need to do to then respond to it. So, I think this is a really important area for which we need to preempt and be quicker off the block to talk about the global response.

Jennifer Elliott:

Thank you. Cecilia, do you want to add anything, or Governor?

Cecilia Skingsley:

No, I can really echo everything that was said. I mean if you look at the various security devices we have, face recognition, thumb recognition, voice, and recognition, I think these companies that provide those sorts of services find themselves in a situation where they can't keep up. We need to think about very different new ways; if you can't know who you're trading with, the foundations of our society are really being challenged. So, we need to come up with some good AI to beat the bad AI.

> Everybody is losing and wiping out their savings. It might not take down a bank, but it takes down a family, it takes down a community, it has a macro-impact, and the scale of it is huge. And so, it's going to take technology, but also a great deal of coordination and a great deal of focus and political will really at the end of the day to manage the problem.
>
> **Jennifer Elliott**
> IMF; Toronto Centre

Jennifer Elliott:

All of you have used the word trust, which is the bottom line of the financial system, isn't it? So, thank you for that. I have one note of optimism, which is I think the new generation is so digitally connected, so native to it that I think the stupid things I do on a phishing email are not going to be replicated by my kids. I think they're way more sophisticated in their use of technology. So, my hope is that financial regulators will hire young people and try and keep up that way.

Anything else from the audience? Great. I think we're ready to wrap up. So, I wanted to say thank you. I mean, here at the Fund, we don't think enough about this, I will say, and I think we think about financial stability, but I'm telling you, industrial scale is what I'm taking away. Everybody is losing and wiping out their savings. It might not take down a bank, but it takes down a family, it takes down a community, it has a macro-impact, and the scale of it is huge. And so, it's going to take technology, but also a great deal of coordination and a great deal of focus and political will really at the end of the day to manage the problem. So, thank you for bringing the different pieces of that together.

I think that was a very effective sort of multidimensional problem laid out for us at least. If we haven't solved it, we've at least laid it out. So, thank you very much.